WeChat Pay callback signature verification bypassed when Host header is localhost

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-33661
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 22:16:29 UTC
Updated	2026-04-01 13:47:23 UTC
Description	Pay is an open-source payment SDK extension package for various Chinese payment services. Prior to version 3.7.20, the

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

EPSS: 0.001700000 probability, percentile 0.381250000 (date 2026-04-01)

Problem Types: CWE-290 | CWE-290 CWE-290: Authentication Bypass by Spoofing

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
3.1	security-advisories@github.com	Secondary	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N
3.1	CNA	DECLARED	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

High

vailability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yansongda	Pay	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Yansongda	Pay	affected < 3.7.20	Not specified

References

Reference	Source	Link
github.com/yansongda/pay/commit/26987ebf789f1e7f0a85febb640986ab4289fd7f	security-advisories@github.com	github.com
github.com/yansongda/pay/releases/tag/v3.7.20	security-advisories@github.com	github.com
github.com/yansongda/pay/security/advisories/GHSA-q938-ghwv-8gvc	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.